UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/706,960	11/06/2000	Scott A. Cluff	MICE-0091-US(00.00902)	8488

7590 01/29/2004

Dan C Hu
Trop Pruner & Hu PC
8554 Katy Freeway
Suite 100
Houston, TX 77024

EXAMINER	
CHU, GABRIEL L	
ART UNIT	**PAPER NUMBER**
2114	

DATE MAILED: 01/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/706,960	CLUFF ET AL.	
	Examiner	Art Unit	
	Gabriel L. Chu	2114	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 November 2003*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Objections

1. Claims 8 and 28 are objected to because of the following informalities:

Referring to claim 8, "the backup storage element" has no antecedent basis. It is understood to refer to "the backup device" of claim 1.

Referring to claim 28, "the first routine" and "the second routine" have no antecedent basis. They are understood to refer to "a first routine" and "a second routine", respectively.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 6145088 to Stevens in view of US 6195695 to Cheston et al. For the rejection of claims 1-10, refer to paper no. 2.

4. Claims 11 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 6145088 to Stevens in view of US 6195695 to Cheston et al. as applied to claims 1 and 10 above, respectively, and further in view of US 5469573 to McGill, III et al. For the rejection of claim 11, refer to paper no. 2.

Referring to claim 31, Stevens discloses that the software is downloaded when a

normal operating system is not operable (Further from line 48 of column 2 (with emphasis), "It is an object of the present invention to provide a means to **enable remote data recovery operations, including, but not limited to, those situations where the normal operating system is not operable**. One embodiment of the invention relates to a method of data recovery comprising the steps of: establishing a communications link via communications hardware from a local computer having a storage device requiring recovery of data to a remote data recovery computer operated by a technician; enabling the technician to interact with the local computer while having access to all data recovery programs which are resident at the remote data recovery computer; and enabling the technician to diagnose and **rectify the data loss of the storage device of the local computer**."). Although Stevens does not specifically disclose the software comprises operating system software, downloading operating system data for recovery is well known in the art. An example of this is shown by Mcgill, III et al., from line 56 of column 1, "Data backup systems are known which restore high capacity hard disks from a digital image of that hard disk, i.e., on a media bit-mapped basis. This type of image restoration may be able to restore an operating system to fixed storage media since the operating system is simply some portion of the total image being restored." A person of ordinary skill in the art at the time of the invention would have been motivated to recover from an image because, from line 58 of column 1 of McGill, III et al., "This type of image restoration may be able to restore an operating system to fixed storage media since the operating system is simply some portion of the total image being restored."

5. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over US 6145088 to Stevens in view of US 6195695 to Cheston et al. as applied to claim 1 above, and further in view of US 6374366 to Maffezzoni. Referring to claim 30, although Stevens does not specifically disclose a BIOS routine to detect a state of the flag, the BIOS routine to access the backup device in response to detecting that the flag indicates the fault, using a BIOS to detect fault and access a backup device is known in the art. An example of this is shown by Maffezoni, from line 8 of column 7, "The SCSI host adapter 103 is preferably a host adapter that is enabled with a special Adaptec, Inc. BIOS that allows users to boot up their computers from the peripheral storage device 104. The special Adaptec, Inc. BIOS is available on Adaptec's AHA-2930CU SCSI Host Adapter and other future host adapters, which are or may be available from Adaptec, Inc. of Milpitas, Calif. In this manner, when a hard disk failure occurs, the special Adaptec, Inc. BIOS will allow the user to boot from the peripheral storage device 104 and continue working until the failure is fixed. In a preferred embodiment, the cartridge 108 media (or the second hard disk) will not only contain valuable data, but also will include the user's operating system (OS) and other important software programs." Further, from line 9 of column 13, "FIG. 4 shows a more detailed flowchart diagram 118 illustrating the operations performed by the intelligent Genesis backup protection system when the host computer system experiences a hard drive failure. The method begins at an operation 252 where the intelligent Genesis backup protection system will automatically prompt the user (via a graphical user interface or text) to re-boot the host computer system from the peripheral storage device, if desired, upon

experiencing the hard drive failure which is detected by a system BIOS. Once re-booted to the peripheral storage device, the method will proceed to an operation 254 where the user can continue uninterrupted working from the intelligently backed-up data using the peripheral storage device, as if no failure had occurred. While the user is working uninterrupted from the intelligently backed-up data of the peripheral storage device, the method will proceed to an operation 256 where the host computer's hard drive will be repaired." Further, from line 32 of column 26, "Upon being enabled, the intelligent Genesis backup protection system will remain in that active state until a failure to the user's hard drive occurs. At that point, the system BIOS will inform the user that an error has occurred with the computer system's hard drive, and the Adaptec BIOS will provide the user with an option to boot the computer system from the peripheral storage device media." A person of ordinary skill in the art at the time of the invention would have been motivated to use a BIOS to respond to a fault because, from line 30 of column 7 of Maffezzoni, it would allow a user to "continue working until the failure is fixed." Further, on PC-compatible computers, a BIOS is the set of essential software routines that test hardware at startup, start the operating system, and support the transfer of data among hardware devices.

6. Claims 12-16 and 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 6145088 to Stevens in view of US 5469573 to McGill, III et al. Referring to claim 12, Stevens discloses detecting if an operating portion of the system has experienced a fault (From the abstract (with emphasis), "establishing a communications link from the local computer containing **the storage device requiring**

recovery of data to a remote data recovery computer operated by a technician."); accessing a backup device to enable communication over a network (Referring to line 55 of column 2 (with emphasis), "establishing a communications link via communications hardware from a local computer having a storage device requiring recovery of data to a remote data recovery computer operated by a technician".); and retrieving over the network (From line 10 of column 3, "In the preferred embodiment, the remote data recovery operating system is sufficiently small to operate directly from its own distribution floppy disk, allowing data recovery operations to proceed in the absence of the normal bootable operating system. It is capable of loading data recovery utility software from either that same distribution floppy disk, or from the remote technician's comparatively vast library of such software, via the communications hardware. In the preferred embodiment, upon loading, the bootable remote data recovery operating system presents a limited number of choices to the local user, allowing the user to input information regarding the nature of the user's data recovery needs and the user's personal data. Once this information has been input, the local user can confirm his intent to have the operating system establish contact with the remote technician via attached communications hardware. This contact can commence the data recovery operation immediately, or, alternatively, may queue the request such that the data recovery operation proceeds at such time as the data recovery technician has had time to review the request and prepare for the data recovery operation. Once the data recovery operation commences, all control of the local computer is released to the remote data recovery technician. The technician is then able to operate the local

computer as though the technician were seated directly in front of it, having access to all data recovery utility software which is available at the technician's site, as well as any which might optionally reside on the data recovery operating system diskette." Further, from line 48 of column 2 (with emphasis), "It is an object of the present invention to provide a means to **enable remote data recovery operations, including, but not limited to, those situations where the normal operating system is not operable**. One embodiment of the invention relates to a method of data recovery comprising the steps of: establishing a communications link via communications hardware from a local computer having a storage device requiring recovery of data to a remote data recovery computer operated by a technician; enabling the technician to interact with the local computer while having access to all data recovery programs which are resident at the remote data recovery computer; and enabling the technician to diagnose and **rectify the data loss of the storage device of the local computer**."). Although Stevens does not specifically disclose the data comprises an image containing user data and an operating system and recovering the system using the image, downloading an image for recovery is well known in the art. An example of this is shown by McGill, III et al., from line 56 of column 1, "Data backup systems are known which restore high capacity hard disks from a digital image of that hard disk, i.e., on a media bit-mapped basis. This type of image restoration may be able to restore an operating system to fixed storage media since the operating system is simply some portion of the total image being restored." Further, from the abstract, "Embodiments of the method include providing the first media by copying the desired operating system files, or all the files, stored on the

storage device to the first media." A person of ordinary skill in the art at the time of the invention would have been motivated to recover from an image because, from line 58 of column 1 of McGill, III et al., "This type of image restoration may be able to restore an operating system to fixed storage media since the operating system is simply some portion of the total image being restored."

Referring to claim 13, Stevens discloses loading a backup software routine from the backup device (From line 65 of column 2, "In one embodiment, the principles of the present invention are achieved by implementing a bootable data recovery operating system which has sufficient functionality to allow communications via communications hardware to the remote technician. The remote technician is further equipped with specialized remote control software which allows communications with the computer running the bootable data recovery operating system via communications hardware. Once the computer under recovery and the remote computer are in communication, data recovery operations on the computer under recovery can proceed under complete control of the remote technician.").

Referring to claim 14, Stevens discloses the backup software routine comprises a browser, the method further comprising executing the browser to access the network to retrieve the data (From line 17 of column 3, "In the preferred embodiment, upon loading, the bootable remote data recovery operating system presents a limited number of choices to the local user, allowing the user to input information regarding the nature of the user's data recovery needs and the user's personal data.").

Referring to claim 15, Stevens discloses executing the backup software routine

to access the network (From line 65 of column 2, "In one embodiment, the principles of the present invention are achieved by implementing a bootable data recovery operating system which has sufficient functionality to allow communications via communications hardware to the remote technician. The remote technician is further equipped with specialized remote control software which allows communications with the computer running the bootable data recovery operating system via communications hardware. Once the computer under recovery and the remote computer are in communication, data recovery operations on the computer under recovery can proceed under complete control of the remote technician.").

Referring to claim 16, Stevens discloses retrieving the data from a backup storage system coupled to the network (From line 10 of column 3, "In the preferred embodiment, the remote data recovery operating system is sufficiently small to operate directly from its own distribution floppy disk, allowing data recovery operations to proceed in the absence of the normal bootable operating system. It is capable of loading data recovery utility software from either that same distribution floppy disk, or from the remote technician's comparatively vast library of such software, via the communications hardware. In the preferred embodiment, upon loading, the bootable remote data recovery operating system presents a limited number of choices to the local user, allowing the user to input information regarding the nature of the user's data recovery needs and the user's personal data. Once this information has been input, the local user can confirm his intent to have the operating system establish contact with the remote technician via attached communications hardware. This contact can commence

the data recovery operation immediately, or, alternatively, may queue the request such that the data recovery operation proceeds at such time as the data recovery technician has had time to review the request and prepare for the data recovery operation. Once the data recovery operation commences, all control of the local computer is released to the remote data recovery technician. The technician is then able to operate the local computer as though the technician were seated directly in front of it, having access to all data recovery utility software which is available at the technician's site, as well as any which might optionally reside on the data recovery operating system diskette." Further, see figure 2.).

Referring to claim 18, Stevens discloses booting from a backup storage device instead of the main storage device if the system has experienced a fault (From line 10 of column 3, "In the preferred embodiment, the remote data recovery operating system is sufficiently small to operate directly from its own distribution floppy disk, allowing data recovery operations to proceed in the absence of the normal bootable operating system. It is capable of loading data recovery utility software from either that same distribution floppy disk, or from the remote technician's comparatively vast library of such software, via the communications hardware."); and using the backup storage device to enable communications over a network to retrieve data to recover the system (From the abstract, "establishing a communications link from the local computer containing the storage device requiring recovery of data to a remote data recovery computer operated by a technician"). Although Stevens does not specifically disclose the data retrieved is image data and wherein the image data comprises user data and an operating system,

downloading an image for recovery is well known in the art. An example of this is shown by McGill, III et al., from line 56 of column 1, "Data backup systems are known which restore high capacity hard disks from a digital image of that hard disk, i.e., on a media bit-mapped basis. This type of image restoration may be able to restore an operating system to fixed storage media since the operating system is simply some portion of the total image being restored." Further, from the abstract, "Embodiments of the method include providing the first media by copying the desired operating system files, or all the files, stored on the storage device to the first media." A person of ordinary skill in the art at the time of the invention would have been motivated to recover from an image because, from line 58 of column 1 of McGill, III et al., "This type of image restoration may be able to restore an operating system to fixed storage media since the operating system is simply some portion of the total image being restored."

Referring to claim 19, Stevens discloses loading a routine from the backup storage device to enable the network communication (From line 65 of column 2, "In one embodiment, the principles of the present invention are achieved by implementing a bootable data recovery operating system which has sufficient functionality to allow communications via communications hardware to the remote technician. The remote technician is further equipped with specialized remote control software which allows communications with the computer running the bootable data recovery operating system via communications hardware. Once the computer under recovery and the remote computer are in communication, data recovery operations on the computer under recovery can proceed under complete control of the remote technician.").

Referring to claim 20, Stevens discloses loading the routine comprises loading a browser (From line 17 of column 3, "In the preferred embodiment, upon loading, the bootable remote data recovery operating system presents a limited number of choices to the local user, allowing the user to input information regarding the nature of the user's data recovery needs and the user's personal data.").

7. Claims 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 6145088 to Stevens in view of US 5469573 to McGill, III et al. as applied to claim 12 above, in further view of US 6374366 to Maffezzoni. Referring to claim 24, although Stevens in view of McGill, III et al. do not specifically disclose in response to the fault, scanning a storage device to determine portions of the storage device that are defective and storing the image in portions of the storage device other than the portions that are defective, scanning a hard drive to avoid bad sectors is notoriously well known in the art. An example of this is shown by Maffezzoni, from line 51 of column 16, "Additionally, the file system repair may include checking an existing file system structure. This advantageously provides an added level of advanced user functionality. If the file system is corrupt, then an attempt can be made to fix it by examining the file system data structures and performing sanity checks. If a fix is possible, then the user will be notified of such and the fix will be attempted. However, in certain circumstances, if the file system is corrupt, then the drive will generally have to be reformatted. The drive repair suite 324 is also capable of communicating with an operating system's ScanDisk. program. The ScanDisk. program can verify the media on the hard drive to determine its condition. In some cases, bad sectors can be mapped out." Further, see figure 5D,

wherein analysis is performed for repair, resulting in a ScanDisk (946) for a subsequent Restore (948). A person of ordinary skill in the art at the time of the invention would have been motivated to perform a ScanDisk because, from line 64 of column 16, it "can verify the media on the hard drive to determine its condition. In some cases, bad sectors can be mapped out."

Referring to claim 25, although Stevens does not specifically disclose setting a flag in response to detecting the operating portion of the system has experienced a fault and a BIOS routine to detect whether the flag has been set, using a BIOS to detect a flag set in response to fault is known in the art. An example of this is shown by Maffezzoni, from line 8 of column 7, "The SCSI host adapter 103 is preferably a host adapter that is enabled with a special Adaptec, Inc. BIOS that allows users to boot up their computers from the peripheral storage device 104. The special Adaptec, Inc. BIOS is available on Adaptec's AHA-2930CU SCSI Host Adapter and other future host adapters, which are or may be available from Adaptec, Inc. of Milpitas, Calif. In this manner, when a hard disk failure occurs, the special Adaptec, Inc. BIOS will allow the user to boot from the peripheral storage device 104 and continue working until the failure is fixed. In a preferred embodiment, the cartridge 108 media (or the second hard disk) will not only contain valuable data, but also will include the user's operating system (OS) and other important software programs." Further, from line 9 of column 13, "FIG. 4 shows a more detailed flowchart diagram 118 illustrating the operations performed by the intelligent Genesis backup protection system when the host computer system experiences a hard drive failure. The method begins at an operation 252 where the

intelligent Genesis backup protection system will automatically prompt the user (via a graphical user interface or text) to re-boot the host computer system from the peripheral storage device, if desired, upon experiencing the hard drive failure which is detected by a system BIOS. Once re-booted to the peripheral storage device, the method will proceed to an operation 254 where the user can continue uninterrupted working from the intelligently backed-up data using the peripheral storage device, as if no failure had occurred. While the user is working uninterrupted from the intelligently backed-up data of the peripheral storage device, the method will proceed to an operation 256 where the host computer's hard drive will be repaired." Further, from line 32 of column 26, "Upon being enabled, the intelligent Genesis backup protection system will remain in that active state until a failure to the user's hard drive occurs. At that point, the system BIOS will inform the user that an error has occurred with the computer system's hard drive, and the Adaptec BIOS will provide the user with an option to boot the computer system from the peripheral storage device media." A person of ordinary skill in the art at the time of the invention would have been motivated to use a BIOS to respond to a fault because, from line 30 of column 7 of Maffezzoni, it would allow a user to "continue working until the failure is fixed." Further, on PC-compatible computers, a BIOS is the set of essential software routines that test hardware at startup, start the operating system, and support the transfer of data among hardware devices.

Referring to claim 26, Stevens in view of McGill, III et al. in view of Maffezzoni teaches the BIOS routine to access the backup device to load a routine for communicating over the network in response to detecting that the flag has been set

(From line 9 of column 13 of Maffezzoni, "FIG. 4 shows a more detailed flowchart diagram 118 illustrating the operations performed by the intelligent Genesis backup protection system when the host computer system experiences a hard drive failure. The method begins at an operation 252 where the intelligent Genesis backup protection system will automatically prompt the user (via a graphical user interface or text) to re-boot the host computer system from the peripheral storage device, if desired, upon experiencing the hard drive failure which is detected by a system BIOS. Once re-booted to the peripheral storage device, the method will proceed to an operation 254 where the user can continue uninterrupted working from the intelligently backed-up data using the peripheral storage device, as if no failure had occurred. While the user is working uninterrupted from the intelligently backed-up data of the peripheral storage device, the method will proceed to an operation 256 where the host computer's hard drive will be repaired.", Further, from line 55 of column 2 of Stevens, "establishing a communications link via communications hardware from a local computer having a storage device requiring recovery of data to a remote data recovery computer operated by a technician".).

8. Claim 17 and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 6145088 to Stevens in view of US 6374366 to Maffezzoni. Referring to claim 17, Stevens discloses detecting if an operating portion of the system has experienced a fault (From the abstract (with emphasis), "establishing a communications link from the local computer containing **the storage device requiring recovery** of data to a remote data recovery computer operated by a technician."); accessing a backup device to

enable communication over a network (Referring to line 55 of column 2 (with emphasis), "establishing a communications link via communications hardware from a local computer having a storage device requiring recovery of data to a remote data recovery computer operated by a technician".); and retrieving data to recover the system over the network (From line 10 of column 3, "In the preferred embodiment, the remote data recovery operating system is sufficiently small to operate directly from its own distribution floppy disk, allowing data recovery operations to proceed in the absence of the normal bootable operating system. It is capable of loading data recovery utility software from either that same distribution floppy disk, or from the remote technician's comparatively vast library of such software, via the communications hardware. In the preferred embodiment, upon loading, the bootable remote data recovery operating system presents a limited number of choices to the local user, allowing the user to input information regarding the nature of the user's data recovery needs and the user's personal data. Once this information has been input, the local user can confirm his intent to have the operating system establish contact with the remote technician via attached communications hardware. This contact can commence the data recovery operation immediately, or, alternatively, may queue the request such that the data recovery operation proceeds at such time as the data recovery technician has had time to review the request and prepare for the data recovery operation. Once the data recovery operation commences, all control of the local computer is released to the remote data recovery technician. The technician is then able to operate the local computer as though the technician were seated directly in front of it, having access to all

data recovery utility software which is available at the technician's site, as well as any which might optionally reside on the data recovery operating system diskette."). Although Stevens does not specifically disclose in response to the fault, scanning a storage device to determine portions of the storage device that are defective and storing the retrieved data in portions of the storage device other than the portions that are defective, scanning a hard drive to avoid bad sectors is notoriously well known in the art. An example of this is shown by Maffezzoni, from line 51 of column 16, "Additionally, the file system repair may include checking an existing file system structure. This advantageously provides an added level of advanced user functionality. If the file system is corrupt, then an attempt can be made to fix it by examining the file system data structures and performing sanity checks. If a fix is possible, then the user will be notified of such and the fix will be attempted. However, in certain circumstances, if the file system is corrupt, then the drive will generally have to be reformatted. The drive repair suite 324 is also capable of communicating with an operating system's ScanDisk. program. The ScanDisk. program can verify the media on the hard drive to determine its condition. In some cases, bad sectors can be mapped out." Further, see figure 5D, wherein analysis is performed for repair, resulting in a ScanDisk (946) for a subsequent Restore (948). A person of ordinary skill in the art at the time of the invention would have been motivated to perform a ScanDisk because, from line 64 of column 16, it "can verify the media on the hard drive to determine its condition. In some cases, bad sectors can be mapped out."

Referring to claim 21, Stevens discloses a main storage device (Referring to line

55 of column 2 (with emphasis), "establishing a communications link via communications hardware from a local computer having **a storage device** requiring recovery of data to a remote data recovery computer operated by a technician".); a backup storage device, and a first routine executable to boot from the backup storage device in case of a system fault (From line 10 of column 3, "In the preferred embodiment, the remote data recovery operating system is sufficiently small to operate directly from its own distribution floppy disk, allowing data recovery operations to proceed in the absence of the normal bootable operating system. It is capable of loading data recovery utility software from either that same distribution floppy disk, or from the remote technician's comparatively vast library of such software, via the communications hardware."), the backup storage device enabling access over a network to retrieve data from a network node to recover the system (From line 65 of column 2, "In one embodiment, the principles of the present invention are achieved by implementing a bootable data recovery operating system which has sufficient functionality to allow communications via communications hardware to the remote technician. The remote technician is further equipped with specialized remote control software which allows communications with the computer running the bootable data recovery operating system via communications hardware. Once the computer under recovery and the remote computer are in communication, data recovery operations on the computer under recovery can proceed under complete control of the remote technician." Further, from From line 10 of column 3, "In the preferred embodiment, the remote data recovery operating system is sufficiently small to operate directly from its

own distribution floppy disk, allowing data recovery operations to proceed in the absence of the normal bootable operating system. It is capable of loading data recovery utility software from either that same distribution floppy disk, or from the remote technician's comparatively vast library of such software, via the communications hardware. In the preferred embodiment, upon loading, the bootable remote data recovery operating system presents a limited number of choices to the local user, allowing the user to input information regarding the nature of the user's data recovery needs and the user's personal data. Once this information has been input, the local user can confirm his intent to have the operating system establish contact with the remote technician via attached communications hardware. This contact can commence the data recovery operation immediately, or, alternatively, may queue the request such that the data recovery operation proceeds at such time as the data recovery technician has had time to review the request and prepare for the data recovery operation. Once the data recovery operation commences, all control of the local computer is released to the remote data recovery technician. The technician is then able to operate the local computer as though the technician were seated directly in front of it, having access to all data recovery utility software which is available at the technician's site, as well as any which might optionally reside on the data recovery operating system diskette."). Although Stevens does not specifically disclose a second routine to identify portions of the main storage device that are defective, and to store the retrieved data in portions of the main storage device that are not defective, scanning a hard drive to avoid bad sectors is notoriously well known in the art. An example of this is shown by Maffezzoni,

from line 51 of column 16, "Additionally, the file system repair may include checking an existing file system structure. This advantageously provides an added level of advanced user functionality. If the file system is corrupt, then an attempt can be made to fix it by examining the file system data structures and performing sanity checks. If a fix is possible, then the user will be notified of such and the fix will be attempted. However, in certain circumstances, if the file system is corrupt, then the drive will generally have to be reformatted. The drive repair suite 324 is also capable of communicating with an operating system's ScanDisk. program. The ScanDisk. program can verify the media on the hard drive to determine its condition. In some cases, bad sectors can be mapped out." Further, see figure 5D, wherein analysis is performed for repair, resulting in a ScanDisk (946) for a subsequent Restore (948). A person of ordinary skill in the art at the time of the invention would have been motivated to perform a ScanDisk because, from line 64 of column 16, it "can verify the media on the hard drive to determine its condition. In some cases, bad sectors can be mapped out."

Referring to claim 22, Stevens discloses the backup storage device comprises a network access routine that is loadable for execution in the system, the network access routine to enable access over the network (From line 65 of column 2, "In one embodiment, the principles of the present invention are achieved by implementing a bootable data recovery operating system which has sufficient functionality to allow communications via communications hardware to the remote technician. The remote technician is further equipped with specialized remote control software which allows

communications with the computer running the bootable data recovery operating system via communications hardware. Once the computer under recovery and the remote computer are in communication, data recovery operations on the computer under recovery can proceed under complete control of the remote technician.").

Referring to claim 23, Stevens in view of Maffezzoni discloses the first routine comprises a BIOS routine (From line 8 of column 7 of Maffezzoni, "The SCSI host adapter 103 is preferably a host adapter that is enabled with a special Adaptec, Inc. BIOS that allows users to boot up their computers from the peripheral storage device 104. The special Adaptec, Inc. BIOS is available on Adaptec's AHA-2930CU SCSI Host Adapter and other future host adapters, which are or may be available from Adaptec, Inc. of Milpitas, Calif. In this manner, when a hard disk failure occurs, the special Adaptec, Inc. BIOS will allow the user to boot from the peripheral storage device 104 and continue working until the failure is fixed. In a preferred embodiment, the cartridge 108 media (or the second hard disk) will not only contain valuable data, but also will include the user's operating system (OS) and other important software programs." Further, from line 9 of column 13, "FIG. 4 shows a more detailed flowchart diagram 118 illustrating the operations performed by the intelligent Genesis backup protection system when the host computer system experiences a hard drive failure. The method begins at an operation 252 where the intelligent Genesis backup protection system will automatically prompt the user (via a graphical user interface or text) to re-boot the host computer system from the peripheral storage device, if desired, upon experiencing the hard drive failure which is detected by a system BIOS. Once re-

booted to the peripheral storage device, the method will proceed to an operation 254 where the user can continue uninterrupted working from the intelligently backed-up data using the peripheral storage device, as if no failure had occurred. While the user is working uninterrupted from the intelligently backed-up data of the peripheral storage device, the method will proceed to an operation 256 where the host computer's hard drive will be repaired." Further, from line 32 of column 26, "Upon being enabled, the intelligent Genesis backup protection system will remain in that active state until a failure to the user's hard drive occurs. At that point, the system BIOS will inform the user that an error has occurred with the computer system's hard drive, and the Adaptec BIOS will provide the user with an option to boot the computer system from the peripheral storage device media.")

9. Claims 27 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 6145088 to Stevens in view of US 6374366 to Maffezzoni as applied to claim 17 above, in further view of US 5469573 to McGill, III et al. Referring to claim 27, although Stevens in view of Maffezzoni does not specifically disclose retrieving the data comprises retrieving image data containing user data and operating system software, downloading an image for recovery is well known in the art. An example of this is shown by McGill, III et al., from line 56 of column 1, "Data backup systems are known which restore high capacity hard disks from a digital image of that hard disk, i.e., on a media bit-mapped basis. This type of image restoration may be able to restore an operating system to fixed storage media since the operating system is simply some portion of the total image being restored." Further, from the abstract, "Embodiments of the method

include providing the first media by copying the desired operating system files, or all the files, stored on the storage device to the first media." A person of ordinary skill in the art at the time of the invention would have been motivated to recover from an image because, from line 58 of column 1 of McGill, III et al., "This type of image restoration may be able to restore an operating system to fixed storage media since the operating system is simply some portion of the total image being restored."

Referring to claim 28, Stevens in view of Maffezzoni discloses a first routine comprises a BIOS routine, and wherein the instructions when executed cause the system to: set a flag in response to the fault; load the BIOS routine to detect whether the flag is set; and cause the BIOS routine to load a second routine in response to detecting the flag is set (From line 8 of column 7 of Maffezzoni, "The SCSI host adapter 103 is preferably a host adapter that is enabled with a special Adaptec, Inc. BIOS that allows users to boot up their computers from the peripheral storage device 104. The special Adaptec, Inc. BIOS is available on Adaptec's AHA-2930CU SCSI Host Adapter and other future host adapters, which are or may be available from Adaptec, Inc. of Milpitas, Calif. In this manner, when a hard disk failure occurs, the special Adaptec, Inc. BIOS will allow the user to boot from the peripheral storage device 104 and continue working until the failure is fixed. In a preferred embodiment, the cartridge 108 media (or the second hard disk) will not only contain valuable data, but also will include the user's operating system (OS) and other important software programs." Further, from line 9 of column 13, "FIG. 4 shows a more detailed flowchart diagram 118 illustrating the operations performed by the intelligent Genesis backup protection system when the

host computer system experiences a hard drive failure. The method begins at an operation 252 where the intelligent Genesis backup protection system will automatically prompt the user (via a graphical user interface or text) to re-boot the host computer system from the peripheral storage device, if desired, upon experiencing the hard drive failure which is detected by a system BIOS. Once re-booted to the peripheral storage device, the method will proceed to an operation 254 where the user can continue uninterrupted working from the intelligently backed-up data using the peripheral storage device, as if no failure had occurred. While the user is working uninterrupted from the intelligently backed-up data of the peripheral storage device, the method will proceed to an operation 256 where the host computer's hard drive will be repaired." Further, from line 32 of column 26, "Upon being enabled, the intelligent Genesis backup protection system will remain in that active state until a failure to the user's hard drive occurs. At that point, the system BIOS will inform the user that an error has occurred with the computer system's hard drive, and the Adaptec BIOS will provide the user with an option to boot the computer system from the peripheral storage device media." A person of ordinary skill in the art at the time of the invention would have been motivated to use a BIOS to respond to a fault because, from line 30 of column 7 of Maffezzoni, it would allow a user to "continue working until the failure is fixed." Further, on PC-compatible computers, a BIOS is the set of essential software routines that test hardware at startup, start the operating system, and support the transfer of data among hardware devices. Further, from line 55 of column 2 of Stevens, "establishing a communications link via

communications hardware from a local computer having a storage device requiring recovery of data to a remote data recovery computer operated by a technician".).

10. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over US 6145088 to Stevens in view of US 6374366 to Maffezzoni as applied to claim 21 above, in further view of US 5469573 to McGill, III et al. Referring to claim 29, although Stevens in view of Maffezzoni does not specifically disclose the retrieved data comprises image data containing user data and operating system software, downloading an image for recovery is well known in the art. An example of this is shown by McGill, III et al., from line 56 of column 1, "Data backup systems are known which restore high capacity hard disks from a digital image of that hard disk, i.e., on a media bit-mapped basis. This type of image restoration may be able to restore an operating system to fixed storage media since the operating system is simply some portion of the total image being restored." Further, from the abstract, "Embodiments of the method include providing the first media by copying the desired operating system files, or all the files, stored on the storage device to the first media." A person of ordinary skill in the art at the time of the invention would have been motivated to recover from an image because, from line 58 of column 1 of McGill, III et al., "This type of image restoration may be able to restore an operating system to fixed storage media since the operating system is simply some portion of the total image being restored."

Response to Arguments

11. Applicant's arguments filed 17 November 2003 have been fully considered but they are not persuasive. In response to applicant's argument that the teachings of

Stevens and Cheston et al. are at odds with each other, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). Further, it is not clear if Applicant understands the nature of the incorporation. Viewing the limitation in claim 1 that is in question, "a storage element containing a flag to indicate if a fault has occurred with the first operational element", although vague, Examiner has interpreted this as an automated means of detecting a need to fail over to a secondary system in case of failure of a primary system. In Stevens, means are provided for activating a secondary system in response to a primary failure, from line 10 of column 3 of Stevens, "In the preferred embodiment, the remote data recovery operating system is sufficiently small to operate directly from its own distribution floppy disk, allowing data recovery operations to proceed in the absence of the normal bootable operating system. It is capable of loading data recovery utility software from either that same distribution floppy disk, or from the remote technician's comparatively vast library of such software, via the communications hardware." However, automatic failover is notoriously well known in the art. It is precisely this deficiency, among other things, that Cheston et al. wishes to cure, from line 66 of column 1 of Cheston et al., "Alternatively, each workstation might be brought back up (or restarted and reloaded with an uncorrupted copy of the executable application and operating system) after a crash from a separate physical media

available at each individual workstation. Two undesirable features relate to having media at each workstation: the cost of distributing and locating the physical media with the executable application and operating system at each of the plurality of workstations and the security of the media from some user removing the media with the executable applications, either inadvertently or as a theft." Whereas the solution provided Cheston et al. has the additional functionality of recovering the application (and the operating system, if desired), again, as previously stated, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art.

Referring to Applicant's argument that there is no teaching within Cheston et al. of a storage element containing a flag to indicate if a fault has occurred with a first operational element, Examiner again references figure 2, elements 55 and 60. Element 55 clearly shows a Boolean indication of the status of the "working copy", i.e., the first operational element. Although this does not explicitly state that this indication is stored in a "storage element", it is inherent that data used in a computer system is stored in a data storing means, whether it be a hard disk, a RAM, a cache, a register, a latch, or some other computer accessible storage. In executing a test to determine whether the working copy of the application and operating system is corrupted, there must be at least one bit or logical state representing "yes" or "no" that corresponds with the state of the working copy so that the computer is able to determine if the working copy is

corrupted. This could be the logical voltage level in the processor that executes the code that implements the test in question. Examiner cites further passages from Cheston et al., from line 24 of column 4, "this test is simple, since current versions of the operating system typically simply "hang" or "crash" and require that the user turn the entire workstation off, then restart the machine, but designs could easily evolve to allow the application and/or operating system to test themselves as to whether either is "corrupted" or not." Further, from line 1 of column 5, "The current workstation operating systems infrequently, but at randomly and unpredictable occasions, cause the working files on the active segments to become corrupted, causing the system to "crash". Today's applications and operating systems then cease to operate and abort with some kind of message to the user that the system has failed. Once the system crashes, then it is necessary for the operator to turn the workstation off and restart the workstation. When the image 0 is executed, it can prompt the user either to indicate that a crash has occurred or that the backup system is to be used, a function which may require a supervisory password." Further, from line 28 of column 5 (with emphasis), "The image from which to boot the workstation after a crash could be indicated by the operator, as described above, with or without a supervisory password. Alternatively, it may be that **the host computer (through the network connection) will indicate the copy of the application to use on boot up, based upon the network knowing which copy of the workstation's program has been used and whether the system "crashed" and needs to be started from a different copy of the application and the operating system**." To further exacerbate the degree of breadth to which the limitation lays claim,

such a "storage element" need not even store a bit, but simply the indication that there is a fault with the first operational element. Indeed, the "system" of claim 1 is not even necessarily a general purpose computer. This could be a node in a telecommunications network, an access point in a power grid, or any other such example that fits in the broad confines of claim 1.

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Gabriel L. Chu whose telephone number is (703) 308-

7298. The examiner can normally be reached on weekdays between 8:30 AM and 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Robert W. Beausoliel, Jr. can be reached on (703) 305-9713. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

gc

ROBERT BEAUSOLIEL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100